



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|---------------------|------------------|
| 10/519,698 | 12/27/2004 | Marc Girault | P1907US | 6941 |
| 8968 7590 05/13/2009 DRINKER BIDDLE & REATH LLP ATTN: PATENT DOCKET DEPT. 191 N. WACKER DRIVE, SUITE 3700 CHICAGO, IL 60606 | | | | |
| EXAMINER | | | | |
| STU, SARAH | | | | |
| ART UNIT | | PAPER NUMBER | | |
| 2431 | | | | |
| MAIL DATE | | DELIVERY MODE | | |
| 05/13/2009 | | PAPER | | |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/519,698

Applicant(s)

GIRAULT ET AL.

Examiner

Sarah Su

Art Unit

2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 March 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☒ Claim(s) 2 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SE/US)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9 February 2009 has been entered. In this amendment, claims 1-6, 8, 10, 12-14, 16-19, 22-23, 26-27, and 30 have been amended.
2. Claims 1-30 are presented for examination.

Response to Arguments

3. With regards to the objection of claim 13, the applicant has submitted amendments, and the examiner hereby withdraws the objection.
4. With regards to the rejection of claim 8 under 35 USC 112, second paragraph, the applicant has submitted amendments, and the examiner hereby withdraws the rejection.
5. Applicant's arguments with respect to claims 1-30 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

6. Claim 2 is objected to because of the following informalities:

- a. In claim 2, line 4: "equal to the public key" should read –equal to the public key–.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 1, 2, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et al. ("A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" and Rivest hereinafter) in view of M'Raihi et al. (US Patent 5,946,397 and M'Raihi hereinafter).

As to claims 1 and 16, Rivest discloses:

generating, at the first entity, a first element of proof (i.e. E) by using a generic number (i.e. M) raised to a first power, modulo the modulus (i.e. n), having a first exponent equal to the public key exponent (i.e. e) multiplied by a random integer (i.e. d) kept secret by the first entity, whereby calculation of said first element of proof is executable independently of the transaction (paragraph 5, line 16; paragraph 6, line 22);
generating, at the first entity, a second element of proof (i.e. public key) related to the first element of proof and dependent on a common

number (i.e. n) shared by the first and second entities specifically for the transaction (paragraph 5, lines 31-47).

Rivest fails to specifically disclose:

verifying, at the second entity that the first element of proof is related through a relationship with a second power, modulo the modulus, of a generic number having a second exponent equal to a linear combination of at least part of the common number and of the public key exponent multiplied by the second element of proof.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rivest, as taught by M'Raihi.

M'Raihi discloses a system and method for cryptography with public key based on the discrete logarithm, the system and method having:

verifying, at the second entity that the first element of proof (i.e. x) is related through a relationship with a second power, modulo the modulus, (i.e. p) of a generic number (i.e. g) having a second exponent (i.e. k) equal to a linear combination of at least part of the common number and of the public key exponent multiplied by the second element of proof (col. 2, lines 4-49).

Given the teaching of M'Raihi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest with the teachings of M'Raihi by verifying a relationship through the use of a linear combination exponent. M'Raihi recites motivation by disclosing that

an exponent is necessary for each signature and creating an exponent using small coefficients in a linear combination would prevent attacks (col. 5, lines 49-52). It is obvious that the teachings of Rivest would have benefited from the teachings of M'Raihi by using an exponent in the form of a linear combination in order to create a signature that is protected against attacks.

As to claim 2, Rivest discloses:

wherein, for identifying the first entity, the first element of proof is generated by the first entity by raising the generic number (i.e. M) to a first power modulo the modulus (i.e. n) having a first exponent equal to the public key exponent (i.e. e) multiplied by a random integer (i.e. d) kept secret by the first entity (paragraph 5, line 16; paragraph 6, line 22);

wherein the common number is chosen randomly from within a security interval $[0, t-1]$ and then sent by the second entity after having received the first element of proof (paragraph 7B, lines 6-8);

wherein the relationship verified by the second entity is an equality relationship between a power of the first element of proof (i.e. E) and the first power of the generic number (paragraph 6, lines 21-36).

9. Claims 11 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest in view of M'Raihi as applied to claims 1 and 16 above, and further in view of Gilbert et al. (US Patent 5,987,138 and Gilbert hereinafter).

As to claim 11, Rivest in view of M'Raihi fails to specifically disclose:

wherein the generic number is transmitted with the public key, the generic number being equal to a simple number raised to a power modulo the modulus with the private key as exponent.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rivest in view of M'Raihi, as taught by Gilbert.

Gilbert discloses a system and method for identification and signature verification, the system and method having:

wherein the generic number is transmitted with the public key, the generic number being equal to a simple number raised to a power modulo the modulus with the private key as exponent (col. 7, lines 19-22).

Given the teaching of Gilbert, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest in view of M'Raihi with the teachings of Gilbert by transmitting a generic number with the public key. Gilbert recites motivation by disclosing that public keys can be based on identity, allowing for a signature public key to identify the user (col. 2, lines 20-24). It is obvious that the teachings of Gilbert would have improved the teachings of Rivest in view of M'Raihi by transmitting a generic number with a public key so that the key can be used to identify the user.

As to claim 17, Rivest in view of M'Raihi fails to specifically disclose:

wherein the communication means is designed to receive the second element of proof (i.e. y) (col. 7, line 51) and wherein the calculation means is designed to calculate the second exponent and said second power of the generic number (col. 7, line 47).

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rivest in view of M'Raihi, as taught by Gilbert.

Gilbert discloses:

wherein the communication means is designed to receive the second element of proof (i.e. y) (col. 7, line 51) and wherein the calculation means is designed to calculate the second exponent and said second power of the generic number (col. 7, line 47).

Given the teaching of Gilbert, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest in view of M'Raihi with the teachings of Gilbert by receiving a second element of proof. Gilbert recites motivation by disclosing that providing for the receiving of an element of proof (i.e. signature) allows for an identification process since public keys can be based on identity, allowing for a signature public key to identify the user (col. 2, lines 20-24). It is obvious that the teachings of Gilbert would have improved the teachings of Rivest in view of M'Raihi by providing for a means to receive an element of proof so that user identification can be performed.

10. Claims 12 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest in view of M'Raihi as applied to claims 1 and 16 above, and further in view of Brickell (US Patent 7,165,181 B2).

As to claims 12 and 18, Rivest in view of M'Raihi does not disclose:

receiving the second element of proof at a third entity;

generating a third element of proof at the third entity by raising the generic number to a power, modulo the modulus, with the second element of proof as exponent;

sending the third element of proof to the second entity;

at the second entity, raising the third element of proof to a power of the public key exponent, modulo the modulus, and multiplying the result thereof by the generic number raised to a power whose exponent is the common number in order to verify the relationship relating the first element of proof to the second element of proof.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Rivest in view of M'Raihi, as evidenced by Brickell.

Brickell discloses a system and method for establishing trust without revealing identity, the system and method having:

receiving the second element of proof (i.e. m') at a third entity (i.e.

Certifying Manufacturer) (col. 5, lines 1-2);

generating a third element of proof (i.e. c') at the third entity by raising the generic number to a power, modulo the modulus, with the second element of proof as exponent (col. 5, lines 2-3);

sending the third element of proof to the second entity (i.e. device) (col. 5, line 3);

at the second entity, raising the third element of proof to a power of the public key exponent, modulo the modulus, (col. 5, lines 3-4) and multiplying the result thereof by the generic number raised to a power whose exponent is the common number in order to verify the relationship relating the first element of proof to the second element of proof (col. 5, lines 5-6; col. 6, lines 18-25).

Given the teaching of Brickell, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest in view of M'Raihi with the teachings of Brickell by using a third entity and signature in the verification process. Brickell recites motivation by disclosing that a cryptographic protocol that achieves anonymity and security requirements without the use of a conventional trusted third party is needed (col. 1, lines 49-52), which can be achieved through the use of a trusted platform module that proves the possession of a signature without revealing the signature (col. 5, lines 8-10). It is obvious that the teachings of Rivest in view of M'Raihi would have benefited from the teachings of Brickell by using a third entity in the verification process in order to maintain security anonymously.

11. Claims 19 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest in view of M'Raihi as applied to claims 1 and 16 above, and further in view of Kasahara et al. (US Patent 6,788,788 B1 and Kasahara hereinafter).

As to claims 19 and 27, Rivest in view of M'Raihi does not disclose:

wherein the common number comprises first and second elementary common numbers, wherein the second element of proof is generated by the first entity by subtracting, from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number, wherein the linear combination equal to the second exponent comprises a zero coefficient for the first elementary common number, a positive unitary coefficient for the second elementary common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof, and wherein, in the verified relationship, the first element of proof is considered with an exponent power equal to the first elementary common number.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rivest in view of M'Raihi, as taught by Kasahara.

Kasahara discloses a system and method for cryptographic communication with high security, the system and method having:

wherein the common number comprises first and second elementary common numbers, wherein the second element of proof is generated by the first entity by subtracting, from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number (col. 16, lines 40-41), wherein the linear combination equal to the second exponent comprises a zero coefficient for the first elementary common number, a positive unitary coefficient for the second elementary common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof (col. 6, line 52), and wherein, in the verified relationship, the first element of proof is considered with an exponent power equal to the first elementary common number (col. 8, line 36; col. 9, line 1).

Given the teaching of Kasahara, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest in view of M'Raihi with the teachings of Kasahara by using small coefficients to create an exponent from a linear combination to be used in the verification process. M'Raihi recites motivation by disclosing that an exponent is necessary for each signature and creating an exponent using small coefficients in a linear combination would prevent attacks (col. 5, lines 49-52). It is obvious that the teachings of Rivest and M'Raihi would have benefited from the teachings of Kasahara by using an exponent in the form of a linear combination in order to create a signature that is protected against attacks.

12. Claims 20-22 and 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest in view of M'Raihi and Kasahara as applied to claims 19 and 27 above, and further in view of Arditti et al. (US Patent 6,125,445 and Arditti hereinafter).

As to claims 20 and 28, Rivest in view of M'Raihi and Kasahara does not disclose:

wherein the second element of proof is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rivest in view of M'Raihi and Kasahara, as taught by Arditti.

Arditti discloses:

wherein the second element of proof (i.e. y) is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus (col. 4, lines 48-50; col. 5, lines 7-8, 16-17).

Given the teaching of Arditti, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest in view of M'Raihi and Kasahara with the teachings of Arditti by disguising the base used to calculate a signature. Arditti recites motivation by disclosing that without the knowledge of the base value, a defrauder cannot correctly

reply to the verifier (col. 3, lines 63-64). It is obvious that the teachings of Rivest in view of M'Raihi and Kasahara would have benefited from the teachings of Arditti by hiding the base value in order to prevent a correct reply from an unauthorized entity.

As to claims 21 and 29, Rivest in view of M'Raihi and Kasahara does not disclose:

**wherein the random integer is less than an image of the modulus via
a Carmichael function or less than a multiple of the order of the generic
number modulo the modulus.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rivest in view of M'Raihi and Kasahara, as taught by Arditti.

Arditti discloses:

**wherein the random integer is less than an image of the modulus via
a Carmichael function or less than a multiple of the order of the generic
number modulo the modulus** (col. 4, lines 48-50; col. 7, lines 4-5).

Given the teaching of Arditti, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest in view of M'Raihi and Kasahara with the teachings of Arditti by using an integer smaller than an image in a verification process. Arditti recites motivation by disclosing that when an integer is close to a multiple of k (following the Carmichael Theorem), then a claimant can be simulated without knowledge of a secret, thus preventing a defrauder from stealing the secret (col. 7, lines 5-9). It is obvious that

the teachings of Arditti would have improved the teachings of Rivest in view of M'Raihi and Kasahara by using an integer smaller than an image in order to allow a claimant to be verified without transferring a secret.

As to claims 22 and 30, Rivest in view of M'Raihi and Kasahara does not disclose:

wherein the first exponent is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rivest in view of M'Raihi and Kasahara, as taught by Arditti.

Arditti discloses:

wherein the first exponent (i.e. T) is calculated modulo an image of the modulus via a Carmichael function (i.e. g) or modulo a multiple of the order of the generic number modulo the modulus (col. 5, lines 7-8).

Given the teaching of Arditti, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest in view of M'Raihi and Kasahara with the teachings of Arditti by using an image in a verification process. Please refer to the motivation as recited above in respect to claims 21 and 29 as to why it is obvious to apply the teachings of Arditti to the teachings of Rivest in view of M'Raihi and Kasahara.

13. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest in view of M'Raihi as applied to claim 1 above, and further in view of Arditti.

As to claims 3 and 4, Rivest combined with M'Raihi discloses:

wherein the common number is chosen at random from within a security interval $[0, t]$ and then sent by the second entity after having received the first element of proof (paragraph 7B, lines 6-8).

Rivest in view of M'Raihi does not disclose:

wherein for authenticating that a message received by the second entity comes from the first entity, the first element of proof is generated by the first entity by applying a hash function to the message and to the generic number raised to a first power, modulo the modulus, having a first exponent equal to the public key exponent multiplied by a random integer kept secret by the first entity;

wherein the relationship verified by the second entity is an equality relationship between the first element of proof and a result of said hash function applied to the message and to the first power of the generic number.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Rivest in view of M'Raihi, as taught by Arditti. Arditti discloses a system and method for public key identification using two hash functions, the system and method having:

wherein for authenticating that a message received by the second entity comes from the first entity, the first element of proof (i.e. $H(y)$) is generated by the first entity by applying a hash function to the message and to the generic number raised to a first power, modulo the modulus, having a first exponent equal to the public key exponent multiplied by a random integer kept secret by the first entity (col. 5, lines 16-18);

wherein the relationship verified by the second entity is an equality relationship between the first element of proof and a result of said hash function applied to the message and to the first power of the generic number (col. 5, lines 29-31).

Given the teaching of Arditti, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest in view of M'Raihi with the teachings of Arditti by using a hash function in order to verify a signature of an entity. Arditti recites motivation by disclosing that security can be increased by being able to perform identity verification without having to reveal secrets (col. 1, lines 11-13), which can be achieved through disguising information (such as through the use of a hash function). It is obvious that the teachings of Arditti would have improved the teachings of Rivest in view of M'Raihi by providing for use of a hash function for verification in order to increase security by performing verification without revealing secrets that could be used maliciously.

14. Claims 5-7, 9-10, 23-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest in view of M'Raihi and Arditti as applied to claims 3 and 4 above, and further in view of Kasahara.

As to claims 5 and 6, Rivest, combined with M'Raihi and Arditti, discloses:

wherein, in the verified relationship, the first element of proof (i.e. E) is considered with an exponent power equal to the first elementary common number (paragraph 6, lines 21-36).

Rivest, combined with M'Raihi and Arditti, does not disclose:

wherein the common number comprises first and second elementary common numbers, wherein the second element of proof is generated by the first entity by subtracting, from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number;

wherein the linear combination equal to the second exponent comprises a zero coefficient for the first elementary common number, a positive unitary coefficient for the second elementary common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Rivest in view of M'Raihi and Arditti, as taught by Kasahara.

Kasahara discloses:

wherein the common number comprises first and second elementary common numbers (i.e. coefficients), wherein the second element of proof (i.e. t_2) is generated by the first entity by subtracting, from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number (col. 16, lines 40-41);

wherein the linear combination equal to the second exponent comprises a zero coefficient for the first elementary common number (i.e. γ), a positive unitary coefficient for the second elementary common number and a positive unitary coefficient for the public key exponent (i.e. A) multiplied by the second element of proof (i.e. v) (col. 6, line 52).

Given the teaching of Kasahara, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest in view of M'Raihi and Arditti with the teachings of Kasahara by using small coefficients to create an exponent from a linear combination to be used in the verification process. Please refer to the motivation as recited above as to claims 19 and 27 why it is obvious to apply the teachings of Kasahara and the use of small coefficients in a linear combination for the verification process to the teachings of Rivest in view of M'Raihi.

As to claim 23, Rivest in view of M'Raihi and Arditti does not disclose:

wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the

common number, wherein the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof, and wherein, in the verified relationship, the first element of proof is considered with a unitary exponent power.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rivest in view of M'Raihi and Arditti, as taught by Kasahara.

Kasahara discloses:

wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the common number (col. 16, lines 40-41), wherein the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof (col. 6, line 52), and wherein, in the verified relationship, the first element of proof is considered with a unitary exponent power (col. 4, line 1).

Given the teaching of Kasahara, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest in view of M'Raihi and Arditti with the teachings of Kasahara by using small coefficients to create an exponent from a linear combination to be used in the verification process. Please refer to the motivation as recited above in

respect to claims 19 and 27 as to why it is obvious to apply the teachings of Kasahara and the use of small coefficients in a linear combination for the verification process to the teachings of Rivest in view of M'Raihi.

As to claims 7 and 24, Rivest in view of M'Raihi and further in view of Arditti, combined with Kasahara discloses:

wherein the second element of proof (i.e. y) is calculated modulo an image of the modulus via a Carmichael function (i.e. g) or modulo a multiple of the order of the generic number modulo the modulus (col. 4, lines 48-50; col. 5, lines 7-8, 16-17) in order to disguise the base used to calculate a signature. Please refer to the motivation recited above with respect to claims 20 and 28 as to why it is obvious to apply the teachings of Arditti to the teachings of Rivest in view of M'Raihi, combined with Kasahara.

As to claims 9 and 25, Rivest in view of M'Raihi further in view of Arditti, combined with Kasahara discloses:

wherein the random integer (i.e. m) is less than an image of the modulus via a Carmichael function (i.e. k) or less than a multiple of the order of the generic number modulo the modulus (col. 4, lines 48-50; col. 7, lines 4-5) in order to allow a claimant to be verified without revealing a secret. Please refer to the motivation recited above with respect to claims 21 and 29 to

as to why it is obvious to apply the teachings of Arditti to the teachings of Rivest in view of M'Raihi, combined with Kasahara.

As to claims 10 and 26, Gilbert in view of M'Raihi further in view of Arditti, combined with Kasahara discloses:

wherein the first exponent (i.e. T) is calculated modulo an image of the modulus via a Carmichael function (i.e. g) or modulo a multiple of the order of the generic number modulo the modulus (col. 5, lines 7-8) in order to allow a claimant to be verified without revealing a secret. Please refer to the motivation as recited above in respect to claim 21 and 29 as to why it is obvious to apply the teachings of Arditti to the teachings of Rivest in view of M'Raihi and Kasahara.

15. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest in view of M'Raihi, Arditti, and Kasahara as applied to claim 6 above, and further in view of Gilbert.

As to claim 8, Rivest in view of M'Raihi, Arditti, and Kasahara fails to specifically disclose:

wherein the random number is greater than the value of the private key in relation to a mathematical problem of a discrete logarithm.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rivest in view of M'Raihi, Arditti, and Kasahara, as taught by Gilbert.

Gilbert discloses:

wherein the random number is greater than the value of the private key (i.e. s) in relation to a mathematical problem of a discrete logarithm (col. 3, lines 35-36).

Given the teaching of Gilbert, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest in view of M'Raihi, Arditti, and Kasahara with the teachings of Gilbert by using a random number that is greater than the private key. Gilbert recites motivation by disclosing that a security level is based on the difficulty of factorizing a number n , which is the product of two large prime numbers (col. 3, lines 33-35). It is obvious that the teachings of Gilbert would have improved the teachings of Rivest in view of M'Raihi, Arditti, and Kasahara by using a random number greater than a private key in order to increase the security level of the signature scheme.

16. Claims 13 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest in view of Kasahara.

As to claim 13, Rivest discloses:

calculation means for generating a first element of proof completely or partly independently of the transaction, said first element of proof being

generated by said prover device by raising a generic number to a first power, modulo the modulus, having a first exponent equal to the first public key exponent multiplied by a random integer kept secret by the prover device (paragraph 5, line 16; paragraph 6, line 22), and for generating a second element of proof related to the first element of proof and dependent on a common number specific to the transaction (paragraph 5, lines 31-47).

Rivest fails to specifically disclose:

communication means for transmitting at least the first and second elements of proof and for transmitting said common number to the verifier device or receiving said common number from the verifier device.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rivest, as taught by Kasahara.

Kasahara discloses:

communication means for transmitting at least the first and second elements of proof (i.e. encrypted plaintext and common key) and for transmitting said common number to the verifier device or receiving said common number from the verifier device (col. 3, lines 43-48).

Given the teaching of Kasahara, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest with the teachings of Kasahara by transmitting elements of proof and a common number. Kasahara recites motivation by disclosing that sharing a common key and ciphertext (i.e. signature) allows for a high degree of

security of communication of information between entities (col. 3, lines 35-41). It is obvious that the teachings of Kasahara would have improved the teachings of Rivest by sharing elements of proof and a common number (i.e. key) in order to provide for a high degree of security in communication between entities.

As to claim 14, Rivest discloses:

wherein the calculation means is, on the one hand, designed to generate a first random number (i.e. d) and to raise a generic number (i.e. M) to a first power, modulo the modulus (i.e. n), having a first exponent equal to the first exponent of the public key (i.e. e) multiplied by the random integer (paragraph 5, lines 39-42; paragraph 6, line 22).

Rivest does not disclose:

wherein the calculation means is, on the other hand designed to generate the second element of proof by taking the difference between the random integer and the private key multiplied by the common number or, where the common number is split into two elementary common numbers, by subtracting from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rivest, as taught by Kasahara.

Kasahara discloses:

wherein the calculation means is, on the other hand designed to generate the second element of proof by taking the difference between the random integer and the private key multiplied by the common number or, where the common number is split into two elementary common numbers, by subtracting from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number (col. 6, line 52; col. 16, lines 40-41).

Given the teaching of Kasahara, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest with the teachings of Kasahara by using small coefficients to create an exponent from a linear combination to be used in the verification process. Please refer to the motivation as recited above in respect to claims 19 and 27 as to why it is obvious to apply the teachings of Kasahara and the use of small coefficients in a linear combination for the verification process to the teachings of Rivest in view of M'Raihi.

17. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest in view of Kasahara as applied to claim 14 above, and further in view of Arditti. As to claim 15, Rivest in view of Kasahara does not disclose:

wherein the calculation means is designed to carry out operations modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rivest in view of Kasahara, as taught by Arditti.

Arditti discloses:

wherein the calculation means is designed to carry out operations modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus (col. 4, lines 48-50).

Given the teaching of Arditti, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rivest in view of Kasahara with the teachings of Arditti by providing for a way to disguise a value used to calculate a signature. Please refer to the motivation as recited above in respect to claims 20 and 28 as to why it is obvious to apply the teachings of Arditti to the teachings of Rivest in view of M'Raihi and Kasahara.

Prior Art Made of Record

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Gennaro et al. (US Patent 6,578,144 B1) discloses a system and method for secure hash and sign signatures.
- b. Hopkins et al. (US 2002/0041683 A1) discloses a system and method for selecting optimal number of prime factors for use in a cryptographic system.

- c. Kocher et al. (US 2008/0104400 A1) discloses a system and method for leak-resistant cryptographic payment smartcard.
- d. Ober et al. (US 2002/0080958 A1) discloses a system and method for cryptographic key management scheme.
- e. Schneier, "Applied Cryptography," 1996, John Wiley & Sons, 2nd Edition, pp. 466-474.
- f. "System for M of M Component Part RSA Digital Signature Generation," (NN97041), IBM Technical Disclosure Bulletin, April 1997.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2431

/Sarah Su/
Examiner, Art Unit 2431